Modernising government

FRAMEWORK FOR INFORMATION AGE GOVERNMENT

Smart cards

CITU

Contents

Executive summary

Ownership and maintenance

This framework is one of a series developed as part of the government's commitment, in the Modernising Government White Paper, to developing an e-government strategy. It was prepared by the Inter-Departmental Steering Group on Card Technology; the Central IT Unit will put in place arrangements for its maintenance on behalf of the Information Age Government Champions.

Other relevant frameworks include those relating to authentication and data standards. The authoritative text of all these documents can be found on the Information Age Government Champions' website, http://www.iagchampions.gov.uk.

Readership

This document is aimed at the public sector, broadly defined, and at those delivering services on its behalf. It should be read by:

- business and IS managers with a requirement to implement or acquire smart card enabled services; and
- technical architects involved in implementing new forms of IT service delivery.

Application, scope and purpose

Smart cards, both single application and multi-application, are potentially an important enabler in encouraging the development of electronic commerce. All government departments should therefore follow this guidance if planning to use smart cards in the delivery of public services, and other public sector bodies are strongly recommended to do so. This will help achieve maximum economies of scale and convenience for card users.

Physically, a smart card normally resembles a credit card, although there are other formats. The distinguishing feature of a smart card, which makes it 'smart', is the inclusion of a microprocessor. This enables the card to process as well as store information, and may enable it to be re-programmed after issue. These capabilities permit a card to be used for both on-line and off-line use, and to carry multiple applications from different issuers. Smart cards can be used for applications such as electronic purses and credit and debit cards, for ID and access control, to hold official documents, for data storage, in mobile phones, and to digitally sign documents to prove integrity and authenticity. Compared to other technologies, they can be resistant to tampering and hacking, and they can provide cryptographic and user-verification functions.

Smart cards may be contact cards where the card reader and the card are in physical contact (as in a bank cashpoint), or contactless, where they communicate remotely, usually at a short distance. Some 'combination' cards have both facilities. Different applications will have different requirements, depending for example on the level of security needed and the speed of access required.

Acquisition issues

In principle, public sector smart card applications can either be added to an existing smart card issued by a third party, or provided through cards issued specifically for the purpose (usually by a commercial service provider). In either case, the strategy must be carefully thought through to maximise potential take-up in the customer base and to ensure that the card scheme is properly administered. The scheme must be made attractive to users in terms of cost, user-friendliness and suitability of all applications which share the card. The card scheme must be designed to ensure that card issue, service levels to cardholders, and withdrawal and cancellation of cards are all covered in detail. Security and liability must also be dealt with. This implies that there must be clear, detailed, and well-designed contracts between the public sector body and the other parties involved.

Data protection and privacy

In order to meet legal requirements including those under the Data Protection Act, and to ensure public confidence in the technology, it is important that all those involved in the issuance of smart cards take account of data protection and privacy issues, and are seen to do so. This includes ensuring that cardholders are kept informed about what information is being held about them, that they have access to that information, and that the technical design of the card and the scheme management are robust and appropriate to prevent unauthorised access to the data. With multi-application cards this will require rigorous separation of the applications and associated data on the card. All these issues will need to be set out in any contracts entered into by a public sector body for the use of smart cards.

Security issues

The security of any card scheme must be considered in the round, and from the outset. It must encompass not just the card itself, but the terminals, back office systems and data transfer techniques. The issues include integrity and confidentiality of data, and authentication and control of access. Schemes must be designed to ensure that compromising one element, such as an individual terminal or card, does not irreversibly break the overall security of the scheme. Guidance from CESG, the National Technical Security Authority, should be sought where appropriate.

Accessibility and reliability

For a card scheme to attract the widest uptake, the system must be designed to allow as many people as possible to use the scheme, including those with disabilities. Cards and readers should be designed with this in mind. The user interface must be clear and user-friendly. The choice of a contact or contactless card will need to be considered. The physical specification of the card must be appropriate to ensure durability and reliability.

A model for public sector cards

In order to maximise the usefulness to the citizen of cards containing public sector applications, a generic model for some of the basic contents is proposed. There are certain user-(i.e. cardholder) controlled details, such as any special needs of the card holder when using the card scheme, which will be applicable to most smart cards. Other applications, such as a digital signature function and a concessions profile, will also be of value in many cases. Including these generic elements will be of benefit to the user, independent of the specific applications also included on the card.

Standards

There are a number of international standards governing various aspects of smart cards and associated infrastructure. However, robust standards have yet to be agreed in some areas, and not all the existing major schemes are fully compliant with recognised standards. It is not possible to realistically summarise these issues in a few sentences, but the issue is considered in detail in Section 6. The annexes to the Framework list those standards which have been agreed, and the areas to which they apply. Appropriate *de jure* international standards should be used where they exist unless there are compelling reasons to the contrary.

1 Introduction

1.1 Ownership and maintenance

This framework is one of a series developed as part of the commitment, in the Modernising Government White Paper, to developing a corporate IT strategy for government. It was prepared by the Inter-Departmental Steering Group on Card Technology, and will be maintained by the Central IT Unit of the Cabinet Office. Comments on this document should be sent to cards@citu.gsi.gov.uk.

Other relevant frameworks include those relating to authentication and data standards. The authoritative text of all these documents can be found on the Information Age Government Champions' website, http://www.iagchampions.gov.uk.

1.2 Who should read this document?

This document is aimed at the public sector, broadly defined, and at those delivering services on its behalf. It should be read by:

- business and IS managers with a requirement to implement or acquire smart card enabled services; and
- technical architects involved in implementing new forms of IT service delivery.

1.3 Application, scope and purpose

As set out in the Performance and Innovation Unit's paper e-commerce@its.best.uk at http://www.cabinet-office.gov.uk/innovations, government regards the deployment of smart cards, including multi-function cards, as a key enabler to the development of electronic commerce and recognises that government applications can act as a key driver towards 'critical mass'.

It is not generally envisaged that central government departments will issue smart cards for public use, although there will be a number of exceptions where existing paper documents are issued in the form of or supplemented by smart cards. Smart cards are likely to be issued by many local authorities and by a variety of private sector organisations. Government believes that the ability to use a smart card issued by the private sector, or any part of the public sector, to access the broadest possible range of public services is of benefit to the card issuer, to the card user and to public service providers. This does not of course imply that a single card will serve every purpose, from bus ticket to credit card to building pass.

In a market with a number of card issuers, some consistency is needed in order to provide the maximum benefit to all parties. This framework is intended to provide a set of standards and guidelines to facilitate technical and commercial interoperability across cards, the associated infrastructure, and card schemes as a whole. It is also intended to provide advice on acquisition issues for public authorities; to ensure that accessibility is an integral part of any card scheme; and to provide guidance on data protection issues.

This document should be read in conjunction with the *Authentication Framework for Information Age Government*, which sets out requirements for enrolment of people and businesses into authentication schemes and describes the circumstances in which government will accept particular types of authentication.

This framework has been produced by the Inter-Departmental Steering Group on Card Technology. The group, whose membership is listed at Annex E, represents a broad range of public sector bodies. The framework is endorsed by the Information Age Government Champions' group. Central government departments and agencies *must comply* with this framework, and it is *strongly recommended* that all UK public sector bodies apply this framework in order to achieve maximum economies of scale, critical mass and convenience for members of the public and business. It is not intended that existing schemes should be required to comply retrospectively but, where practicable, these guidelines should be followed in any extension or replacement of an existing scheme.

Authorities should:

- follow the advice given in this framework regarding management, acquisition, data protection and privacy and accessibility to card data and the scheme as a whole;
- comply with the relevant parts of the technical standards set out in this document, or ensure compliance by their suppliers;
- incorporate the data elements identified as 'core' in Section 6 of this document; and
- if incorporating elements serving the same function as the 'optional' data elements described in this document, follow the standards for those elements set out in this document.

This framework is not specifically concerned with the issue of smart cards in respect of government-to-government transactions. Nevertheless, much of the guidance contained in this document is equally applicable to these circumstances and should be followed by departments issuing cards in these situations.

1.4 Types of smart card and their benefits

There are essentially two types of smart card: contact and contactless. Contact cards must be in physical contact with the card reader in order to be read. Contactless cards communicate via radio signals and depending on the type, may operate at a distance from the reader varying from a few millimetres to many metres. A third type of card, the combination card, may operate in both contact and contactless mode.

Contact cards, with the exception of some used in mobile phones and for other specialist applications, are normally the same size as a credit card (technically, this is known as an ID-1 card). Contactless cards may be credit-card sized, but are also found in other formats such as key fobs.

Smart cards are also found in smaller physical formats and as dedicated, single application cards which may incorporate only a dedicated function Application Specific Integrated Circuit (ASIC).

All smart cards have a microprocessor, which means that;

- the card can process, rather than just store information;
- the card may be programmed and in its upgradeable, multi-application form, new applications may be added after issue; and
- the card can store comparatively large amounts of information (by comparison with, say, a magnetic-stripe card) and can control access to that information.

Smart cards have a number of generic benefits and any smart card scheme should seek to gain maximum advantage from these – though not all will apply to every application.

- Off-line use. Smart cards act as portable, rewriteable data stores and are therefore particularly suitable for off-line use. This can reduce infrastructure costs and telecommunications charges, and make mobile use practical. However, a careful backup strategy is required to cater for card loss, in particular to ensure than any central database information is kept in step with the data on the card.
- On-line use. Conversely, smart cards can facilitate secure access to a range of on-line services. This can make a range of data management problems easier than with ‘off-line’ use.
- Multiple use. A single card may be used for multiple purposes. This may occur in a number of ways:
  - single function, multiple use – the card may perform a single function, such as making a payment, in a variety of situations;
  - multiple function, multiple use – the card may hold a number of discrete sets of data, each serving a different purpose;
  - multiple applications – the card may hold a number of intelligent applications, each performing a different function. In principle, applications may be added or removed during the card’s life cycle.

If a number of parties are able to agree to share a card and/or the associated infrastructure, then the cost to each party may be reduced and the number of locations where the card can be used increased. However, such schemes will only be practical if the legal, management, technical, cultural, and security and other issues involved are considered in detail from the outset and can be clearly and satisfactorily resolved. These topics are considered in more detail elsewhere in this paper.

- Security. Smart card security is not infallible, but smart cards are difficult to counterfeit compared to most other card technologies, and their processing power and storage capacity provides various security benefits.
  - Cardholder verification: the card may use a built-in PIN or biometric template to prevent misuse if lost or stolen. The use of biometric identification may also prevent misuse through cards being lent or borrowed: whilst it is possible to acquire a PIN, only the legitimate user possesses a biometric characteristic.
  - Card and terminal verification: the card and the terminal may mutually authenticate to ensure each is genuine.
  - Access control and tamper resistance: data intended for different purposes may be stored in discrete parts of the card's memory, and accessed only by authorised persons or applications. Sharing of data between card applications is also possible in principle, but this needs very careful design, as there are legal and technical hurdles to be overcome.
  - Cryptographic functionality: the card may have sufficient processing power to carry out a digital signature function, without releasing the private signing key to the terminal. This allows the card to be used in an insecure environment, and in multiple terminals, without breaching the integrity of the signature system. This function may be performed within a public-key infrastructure scheme, potentially enabling use of the digital signature function for a wide variety of secure transactions.

1.5 Typical smart card applications

Smart cards have a variety of applications.

- Electronic purses and stored value cards, including:
  - prepaid schemes where a payment is made in advance, the prepaid value being stored on the card and deductions made as goods and services are consumed, for example, public telephone cards, public transport tokens, and cards for minor items of expenditure in closed environments; and
  - 'open' purse schemes, where the card effectively stores cash value. (Such schemes are subject to specific banking regulation.)
- Loyalty cards.
- Identification and access control. Cards may be used to identify either employees or members of the public and to provide access to buildings or computer systems.
- Official documents. Some official documents may be issued in the form of smart cards, at least as an alternative to paper documents.

- Digital signature. Cards may be used by an individual or an organisation to digitally sign electronic messages, thereby providing proof of authenticity and integrity.
- Data storage. Cards may be used to hold significant amounts of information, which may be fairly static – such as the holder's name and address, personal preferences or special needs – or dynamic, such as a record of attendance at classes.
- Mobile telephony. GSM smart cards identify the subscriber to the telephone system and store information such as frequently called numbers. The cards may usually be moved from phone to phone.
- Credit and debit cards. The smart card chip provides greater protection against counterfeiting and may in due course be used to reduce fraud in remote transactions, such as across the Internet, and for cardholder verification. In the UK, 'EMV' (Europay/MasterCard/Visa) smart credit and debit cards are already being issued. (However, at present, banking specifications affect full interoperability of bank-issued cards and prevent the debit/credit application from being loaded on to cards which have not been issued by a bank.)
- Access to on-line data and services.
- Public sector services. Cards may be used for a range of public-sector-specific applications, such as library cards or learning cards.

2 Acquisition

2.1 Introduction

Where a requirement for a smart card has been identified, there are in effect three acquisition options:

i) make use of an existing or planned card scheme, without adding an application or data;

ii) 'rent space' on an existing card; or

iii) issue cards and, where appropriate, offset the cost by making space or use available to others.

Option (i) may be applicable where an existing card provides all the necessary data and functionality, in an acceptable format, and where technical, commercial and security issues can be agreed. A service provider might, for example, agree to accept a privately issued digital-signature card as sufficient proof of identity for its own purposes.

Whichever option is chosen, the issues set out below should be considered, in addition to the guidance elsewhere in this framework on data protection, security, accessibility and standards.

2.2 Card volume

In order to ensure that the highest possible proportion of service users both obtain and subsequently choose to carry the card, it is important that:

- the other applications on the card will benefit and appeal to the intended users and will frequently be used by them;
- the scheme is user-friendly to the cardholder. This will include the design of the user interface, ease and clarity of undertaking transactions, and accessibility of terminals;
- any charge levied on users for the card as a whole, or for individual applications, is proportionate to the value which the card offers them; and
- Any other applications on the card will not be perceived as incompatible with the intended application. Users may be unwilling to hold a card if, for example, they fear that sensitive information held on the card for one purpose will be made available when they present the card for another purpose.

In other words, the benefits of using a smart card must be evident to the cardholders, and any concerns addressed.

2.3 Card issue and management

- The card issuer must be willing and able to issue the card to all members of the target user group. If, for example, a card is marketed on the basis of an exclusive brand, or is only available to those with a robust credit rating, it may be unsuitable for many public service applications.

- There must be a satisfactory agreement between the parties about card loss and card withdrawal. In what circumstances will a card, or an individual application on the card, be withdrawn? There must be clear procedures for withdrawing or cancelling applications, and in extremis for cancelling the whole card in the event that security is compromised or the card is misused. It must be clear how public services will be provided if a card is lost, withdrawn or stolen. These requirements may raise complex management issues with multi-application cards.

- There must be clear responsibility for managing the customer relationship and for providing help-desk services. Service levels to the user in terms of availability of card readers and response times need to be clearly established. The cardholder must know whom to contact in case of card loss or other contingencies. Branding of the card must be addressed.

- There must be a clear strategy for card replacement. In the case of multi-function cards, this may involve reloading the card with back-up data from disparate sources, and it must usually be possible for the cardholder to achieve this via a single operation. A decision may need to be made as to whether or not a central back-up agency is allowed to read sensitive information on the card for back-up purposes, and whether it is allowed to store security-sensitive data. If so, a public authority will need to be satisfied of the standing of the agency, and that its management, operational and security procedures are appropriately robust.

- There must be a clear procedure for card or application withdrawal/cancellation on the holder's death and, where appropriate, in other circumstances such as emigration.

- There must be clear understanding of the responsibilities of the card issuer and of the application provider. In the case of multi-function cards the issuer will usually, but not always, provide and manage the network and systems for loading (including dynamic downloading), updating and deleting application modules on the card (including security management). The issuer is unlikely to take any responsibility for the quality of the applications provided by third parties, but will merely ensure that the downloaded application module is an accurate copy of the master module submitted by the application provider. The issuer should provide a mechanism to block and unblock an application by means of a 'hot list' distributed to key points in the terminal network – such a mechanism is likely to be issuer-specific.

2.4 Cardholder enrolment

All organisations enrolling cardholders must follow appropriate procedures. In particular, if the card itself or an application on the card is to be used to vouch for an individual's identity or status, the issue process must be carefully controlled. This matter is considered further in the authentication framework.

2.5 Risk and liability

Careful allocation and mitigation of risk will be required in any card scheme, and authorities should carry out a formal risk assessment. The potential risks include the following.

- Commercial failure of the scheme. It must be recognised that, where a public service application 'piggy-backs' on a commercial card scheme, failure of the commercial scheme will make cards and infrastructure unavailable to the public sector scheme. This leads to a risk of service unavailability and nugatory investment in software and systems. Where there is a contractual relationship between an authority and a commercial supplier, success criteria will need to be agreed at the outset.

- Lack of takeup by cardholders. Card schemes may completely fail to meet their objectives unless a critical mass of users adopts the card. Careful attention must be paid to the parties' responsibilities for marketing the card, and the contract carefully structured to provide appropriate incentives to all parties.

- Lack of acceptance by service providers. The usability of the card may depend upon the availability of readers, and in some cases on the presence of trained staff, on third party premises.

- Technical failure – of the card itself, the infrastructure or systems integration. All components of the scheme must be of demonstrable quality. In particular, the quality of the card software must be high, and its design must follow fault-tolerant best practice.

- Breach of security. Security must be considered holistically, and includes the technical security of the card, infrastructure and back office systems, the effectiveness of the cardholder verification method in real-world use, and the effectiveness of the audit, accounting and procedural controls applied to the overall scheme.

- Unauthorised access to or use of a card or cardholder data, to the cardholder's detriment. Liability to compensate the cardholder, and the limits on the cardholder's liability, must be clearly established.

- Damage to a cardholder through reliance being placed on inaccurate or outdated information held on the card. There must be clear procedures for verifying information and for ensuring information is kept up to date, and clear establishment of liabilities and procedures for providing the cardholder with access to the data and with the ability to correct inaccurate entries.

- Damage to a third party through misuse of the card by the cardholder. The rights and responsibilities of the cardholder, and liabilities of the parties, must be clearly established.

- Inadequate enrolment procedures, where accurate establishment of the user's identity or status or the prevention of duplicate card issue is important.

Before a scheme is entered into, the business model in respect of funding and fee arrangements, contract duration, incentives and similar matters will need to be contractually agreed between the parties.

2.6 Contract expiry/termination

Careful consideration must be given to ensuring continuity of service on termination or expiry of the contract, and to ensuring that the authority is in a position to engage an alternative contractor if required.

Issues to be considered include:

- ownership of and access to intellectual property including source code and data.
- arrangements for co-operation between the outgoing and incoming service provider.
- agreement of appropriate standards to ensure that applications may be ported to a new platform without undue difficulty.

2.6 Interoperability and technical standards

The following technical issues also need to be borne in mind.

- The majority of multi-application card platforms adhere to international standards (primarily ISO/IEC), but other contact-interface platforms are available, including banking applications. In particular, banking rules usually require that the entire card and the terminals be type approved for the purpose, and for security reasons contactless cards in debit/credit card applications are not normally permitted.

- Mobile phone (GSM) cards are beginning to offer multi-application functionality, but GSM specifications are in places different from ISO/IEC, and application portability from an ISO platform to a GSM platform may be difficult. GSM also has tight restrictions on power consumption, so that certain strong security functions are not yet available on a GSM platform.

2.8 Card type

The type of card (contact, contactless or combination) must be appropriate to the application and to the way in which the card will be used. Contact cards will be the norm in PCs, interactive television, ATMs and retail outlets. Contactless readers will be the norm for public transport, and have advantages in terms of convenience and card life for building-access control.

3 Privacy and data protection

3.1 Policy

It is important that data-protection issues be considered from the outset of the introduction of any smart card scheme. This is necessary in order to ensure compliance with legislative requirements and government policy and, equally importantly, to maintain public confidence. This is particularly the case where perceived or actual risks to data protection may be heightened by the deployment of unfamiliar technology.

The following is an outline agreement on data protection, to be agreed between the authority and the card/application issuer. The totality of the requirements below will apply in cases where the card issuer is also an application issuer. In some cases the card issuer may not have any of its own applications on the card, and for multi-application cards, most applications will be owned by a party which is not the card issuer. The precise roles and responsibilities of the different parties in meeting the requirements outlined below will need to be determined contractually in each case, albeit the issuer is likely in all cases to have a key role. Technical issues, such as encryption techniques, may need to be made explicit in the contract.

This of course means that where a public authority uses a smart card, as an application owner and/or as an issuer, it will itself have specific responsibilities (including those in the Data Protection Act) to ensure that it meets its obligations under the following section. Again, these will have to be clearly borne in mind from the outset of the authority's involvement, and will normally be made explicit in the contract(s) with the other parties.

3.2 Outline Agreement

General

The contractor will comply with Annex C (Data Protection and Retention Policy) of Channels for Electronic Service Delivery: Draft Operating Licence, published by the Central IT Unit (http://www.citu.gov.uk).

Information

The contractor shall implement procedures to ensure that information held on the smart card, and on any associated data processing or storage system, is accurate, current, and the minimum necessary for the purpose. When no longer required, information shall be purged from the card and associated systems.

The contractor shall ensure that information given for one purpose is not used for any other purpose, or passed to any third party, without the subject's informed consent. (Under careful controls, access may be granted to a back-up service provider.) This means that authorities should only have access to information on the card necessary to carry out transactions with that authority.

The contractor shall ensure that the cardholder is informed of:

- what information is being held;
- the purpose for which it is being held; and
- when it is being passed on.

Subject access

The contractor shall provide for cardholders to obtain access to all information held about them on the card and any associated system, in accordance with the requirements laid down in UK data protection legislation at the time of the request. The data subject shall not have to make multiple requests to multiple service providers, and pay multiple fees, in order to access the totality of the information.

Security

The contractor shall ensure that the card itself, and the associated systems, are sufficiently secure to protect the information held from unauthorised access, modification or deletion. This will include ensuring security during distribution and loading of data.

The contractor shall ensure that information on the card is securely segregated, so that information associated with one application or purpose cannot be accessed or interfered with by other applications. There may be circumstances in which certain data can be shared between applications, which will simplify matters. However, this will need to be approved in advance by the cardholder, the application owner(s) and the issuer.

Cardholder verification

The contractor shall ensure that the card has an effective method of cardholder verification, and that the cardholder is successfully verified to the card before sensitive information is released or the card used to authenticate the holder for the purpose of any binding transaction. The cardholder verification system shall use PINs, biometrics, or other methods, used singly or in combination subject to the requirements of the scheme, technical robustness and user acceptability.

4 Security issues

The implementation of security measures is always a matter of balancing cost and inconvenience against the likelihood of the information held being compromised and the potential maximum impact of any such compromise. For example, complex cryptography increases card cost and transaction times. It should be noted that the overall level of security required on a card will be determined by the individual application with the highest security requirements.

It is important to appreciate that card security is not infallible. As cards are easily lost or stolen, it must be assumed that potential attackers will be able to devote considerable time and resources to attempting to break into a card (by destructive or non-destructive means) or to duplicate it, if they can gain sufficient benefit by so doing.

It is hence important to design any card scheme so that the benefit to be gained from obtaining supposedly secret information from a particular card is minimised. Any scheme whereby breaking into a single card can jeopardise the security of the entire scheme is inherently vulnerable.

A holistic view must be taken of scheme security, and schemes designed so that:

- the physical security of the card is complemented by appropriate accounting and audit measures;
- the likelihood and potential maximum impact of compromise of the information held on the card is minimised;
- where possible and appropriate, information is split between the card and the system such that compromising the integrity of either does not breach overall security;
- all system components, including terminals, communications links and 'back-office' systems, are appropriately protected; and
- management systems provide for timely blocking of cards suspected of participating in security breaches.

Authorities should consider:

- requiring that the card scheme be covered by a security management system independently certified as complying with BS 7799;
- requiring that the card itself, the operating system and/or the applications be evaluated using the Common Criteria for Information Technology Security (ISO 15408). (In practice it is likely that ITSEC standards will be used in many cases, at least in the short term); and
- requiring that the card reader and method of communicating with the cardholder are implemented within a secure 'trusted terminal' architecture.

This is not an exhaustive list of the possible security issues. Authorities should consult the national technical security authority, CESG, if in any doubt.

5 Accessibility and reliability issues

5.1 Introduction

Accessibility is a clear requirement for all public services, and investments in better accessibility can often be cost-effective through increasing the market for a service and by encouraging a greater proportion of the population to use automated, self-service systems rather than counter staff. Many accessibility measures impose minimal extra cost, particularly if designed-in from the start. Some measures, in particular those to assist the disabled when using public and workplace systems, may be needed to meet legal obligations.

Smart cards themselves, and the devices with which they interface, must be as easy to use as possible. Smart cards may also hold information about the user's particular requirements – for accessibility, type of interface, etc – enabling a better service to be provided.

Reliability of cards and terminal equipment is essential both for public acceptance and for the proper provision of services. Management of smart card schemes – from procurement through to delivery and user support – must be governed by performance and reliability specifications and targets, and by diligent monitoring of quality.

5.2 Standards issues

The following issues are partially covered by European or international standards, which are listed in the annexes to this paper.

5.2.1 Physical design of cards

It should be possible to orient contact cards by touch. This can be achieved by placing a notch in one edge of the card, as has been the practice with telephone cards for some years.

For the visually impaired, identification of one card amongst several different cards remains an outstanding issue. The financial sector prefers to use embossing, but many smart card readers cannot accept embossed cards.

5.2.2 Special requirements

Special requirements – such as for more time to complete an action, a different operating mode for the terminal, or assistance to access a building – can be encoded on the card and used to assist in providing better service.

5.2.3 Terminal devices

Careful design of the terminal itself, of the user interface, and of the transaction process can all make services easier to use without adding significantly to cost. It is also important that the transaction process is carefully designed so that users are made aware of their legal obligations and of any charge involved; are able to cancel the transaction at any point before completion; and can obtain a receipt. It will usually be necessary for the user to be able to read much of the data stored on the card at the point of use – for example, how many units of an entitlement remain, or the date when an application expires.

For public service terminals and in the workplace, there are legal requirements for assisting those with special needs. New-design public service kiosks (including ATMs) should be able to make available features such as large-size characters on the display, by obtaining information about the user's requirements from the card.

5.3 Other considerations

5.3.1 Card type

The type of card interface used – contact or contactless – should reflect the circumstances. In practice, the choices available to the application provider often result in a trade-off between functional requirements and technology constraints. Contactless cards are easier for certain groups to use as they need not be placed in a slot, and are essential for high-throughput ticket gates. However, the very short transaction times associated with contactless cards, which may be in communication with the reader for less than half a second, makes them unsuitable for some applications, particularly where the card must carry out complex cryptographic functions. Some application providers, particularly in the financial sector, will not permit their application to operate over a contactless interface due to a perceived security risk associated with the ease with which communication can be monitored.

Contact cards are in widespread use in the finance and other sectors and PC, interactive TV, retail outlet and many other readers are of the contact type. Careful design of the interaction between terminal and user can make contact cards easy for very nearly all groups to use.

Combination cards have a dual (contact and contactless) interface. It is expected that they will be deployed in volume in the near future, providing in particular public transport functions across the contactless interface and an e-purse or region/town/city card function across the contact interface.

5.3.2 Compliance tests

Card schemes requiring high security and/or high usability have often found it necessary to set up their own compliance tests. Such tests lead to cards, terminal equipment and management systems being type-approved, usually only for one particular scheme. In the absence of a full set of standards for terminal equipment, these type-approval tests have become a key factor in ensuring quality of service.

5.3.3 Reliability

The card issuer should ensure that the card is purchased to a specification appropriate for the target cardholder population, operating environment, and required lifespan. The application providers should in turn satisfy themselves that the card platform will deliver the required in-service life.

Physical reliability of a smart card is dependent on the materials and processes used to manufacture it. The reliability of the micro-module (the card integrated circuit and the contact area or ‘stamp’) is similarly dependent. Thus a disposable telephone card and a five-year-life building-access card are manufactured using quite different processes and materials.

Electrically, the working life of the integrated circuit is usually dependent on the number of write accesses to permanent (non-volatile) memory, but recent advances in technology have taken the failure point in normal use well beyond the required operating life of a consumer or government card.

There are no standards for card reliability, but there are some standards for test methods, and the tests in those standards can be adapted to turn them into accelerated life-tests. The smart card industry has also developed further life-test methods.

6 Content and technical standards

6.1 Introduction

Technical standards in respect of smart cards and their associated infrastructure are complex, and in a number of areas fully developed and universally accepted standards have yet to be achieved. This section of the Framework and the relevant Annexes therefore cover the issues in some detail, in order to appraise the reader of the potential complexities in implementing a card scheme. It is recognised that not every element will be relevant to all readers of this Framework.

6.1 Objectives

This Framework's aims include:

- allowing the maximum scope for innovation;
- ensuring interoperability of cards and terminals when used for public sector functions;
- avoiding 'lock-in' to a particular supplier;
- maximising usability; and
- ensuring appropriate levels of security.

To satisfy these aims, a minimum set of standards and specifications is required.

6.2 Overview of standards issues

Base standards are required to set the parameters within which products and services may be implemented. Those parameters may include minimum requirements for non-interference and a greater or lesser degree of interoperability. Within the set parameters, specifications and application standards reduce the number of possibilities at the implementation level to a manageable subset, and thus facilitate interoperability. Specifications may include enhanced and additional features, and so are often the precursor of new and improved standards. Specifications are also the way to set performance levels.

Proprietary supplier specifications may be offered for standardisation in areas where standards are not available or existing standards are inappropriate. This standardisation route may be used to allow innovation while avoiding lock-in to a single supplier for future enhancements and replacements. Implicit in standardisation is the agreement of the owner of the intellectual property to licence the technology at reasonable cost.

Much smart card standardisation work, particularly for the hardware and for security, is dealt with jointly by the International Standards Organisation (ISO) and the International Electro-technical Commission (IEC). The European Standards Committee (CEN) does not duplicate work already undertaken by ISO/IEC but concentrates on areas where there is a consensus (or a will to consensus) in Europe that is lacking elsewhere. For example, at the data model, application, and user- interface levels, European standards produced by CEN supplement the basic International Standards. For cards used in digital mobile phones, the European Telecommunications Standards Institute (ETSI) produces specifications which have become de facto standards, but some mobile phones also feature a second, non-ETSI card slot designed for non-telecommunications functions.

Standardisation has always concentrated on cards, with the design of terminals or readers for smart cards regarded as derivative, so that development has been fragmented. Numerous attempts, public and private, have been made to encourage scheme developers and terminal equipment suppliers to collaborate on underlying technology in order to compete in the market, and the development of multi-application card platforms now makes that approach essential. Interoperability at this level is a global issue, but the drive to address it is in part regional and in part confined to single countries.

For contact interface applications, the concept of the industry-standard terminal is only now emerging, driven by European standardisation initiatives. For retail systems, there is UK industry collaborative work endorsed by the British Retail Consortium.

For transport applications, the 1998 Integrated Transport White Paper endorsed interoperability across different types of public transport. This is likely to be realised by the deployment of multi-standard contactless interface terminal equipment and a mix of combination (dual interface) and basic contactless cards.

6.3 Application of standards to public service cards

Organisations procuring smart cards should consider standards at five levels: physical and card-to-terminal interface; user interface and terminal equipment; physical security and in particular, microprocessor and crypto-controller security; operating system; and application and content standards.

This framework presents preferred standards at some of these levels, and sets out the issues for contracting authorities at other levels. The preferred standards are intended to reflect general industry practice as far as is practicable: compliance with them will facilitate – but not in itself guarantee – interoperability.

6.3.1 Physical and card-to-terminal interface standards

(a) Objectives

The objective of agreeing standards at this level is to:

- ensure that cards may be used in conjunction with any industry-standard terminal and that the contents may be accessed;
- ensure ease of use – by making cards a standard size, and providing a physical feature (tactile identifier) to assist visually impaired people; and
- provide common test methods for assessing quality.

Physical and interface standards cover the card's dimensions; location and layout of contacts; power consumption; electrical and communications interfaces; and so forth. Test standards at this level provide ways of measuring characteristics and performance, including some mechanical reliability parameters. The setting of physical reliability targets is a matter for individual card issuers, who will need to determine appropriate values to meet service-level requirements.

(b) Standards issues

There is a choice of implementation options for card communications protocols, but, to allow interoperability, terminals should be designed to work with cards that implement any or all of the available options. The standards allow for some latitude for negotiation between terminal and card when they first communicate. The Europay Mastercard Visa (EMV) specification, however, requires material beyond that contained in the standards to ensure interoperability, and this is likely to be a more general issue (see Annex B re ISO/IEC 7816).

Physical and interface standards are well defined for contact cards, and for certain types of contactless cards, by ISO/IEC. Standards for card orientation aids are defined by CEN. However, there are transitional issues.

- In the banking sector, most card issuers adhere to EMV specifications. That, coupled with banking-scheme rules about using only banking sector approved equipment, currently points the developer of a new application to consider whether it be mounted on a bank-issued, EMV card platform, or on another issuer's ISO card platform.

- The standard for the set of contactless interfaces which is being used worldwide for high volume public transport applications (proximity cards) is, as yet, incomplete. As a result, proximity cards are likely to continue to be deployed to industry specifications, most of which are now available for standardisation – but there may prove to be a continuing lack of complete harmonisation between the deployed population of cards and terminals and the eventual ISO standard.

- Card-orientation notch standards are currently subject to discussions on a global scale because of conflicts with the large installed base of card personalisation equipment.

- Existing ‘closed’ commercial schemes may have elements derived from ISO standards, but may not be fully ISO compliant to enable full interoperability in accordance with these standards.

- There are industry consortia collaborating on common terminal specifications (in particular the PC/SC consortium). As yet however, universally acceptable and robust specifications remain to be produced.

- Not all trusted terminal developments are fully ISO compliant.

(c) Preferred standards

Preferred standards are listed at Annex B.

6.3.2 User interface and terminal equipment standards

(a) Objectives

It is desirable to present users of card-operated devices with a consistent user interface, and to make terminal equipment accessible to the widest possible group of users.

(b) Standards issues

There is little standardisation of public-use terminal equipment, except by way of industry specifications for individual schemes, mainly in the financial sector. More-general industry consortia (eg PC/SC) have made some progress, but most of the work revolves around the application program interface (API) within the terminal or in an associated host computer system. The retail sector has been the most active in this area, and is largely concentrating on influencing financial card scheme owners to accept a terminal architecture suitable for handling, through a single slot, all the cards that the large retail chains may wish to accept. This is the closest approach yet to defining the industry-standard terminal.

The European Commission is promoting work in the e-commerce field, and the work that it sponsors is relevant to public sector transactions both with the public and with business. It is currently running a ‘horizontal’ work programme, aimed at identifying and unifying common features of self-service transactions.

(c) Preferred standards

Guidance on these issues is given at Annex B .

6.3.3 Physical security

(a) Objectives

The need to set standards for physical security depends upon the application to which the card is being put and the benefit to the attacker of being able to break a single card.

As has been noted, smart cards cannot be considered entirely secure against attack: there are a variety of possible attacks on cards, and a variety of countermeasures. Both attacks and countermeasures are continually being developed. Card schemes should be carefully designed to ensure that the benefit to be gained from breaking the security of a single card does not justify the effort which an attacker would have to employ.

(b) Preferred standards

For most government-business and government-citizen transactions - where the card is acquired as part of a service contract - authorities are unlikely to wish to specify standards for physical security of the card, and should instead rely on careful scheme design and on careful allocation of risk. Where the physical security of the card is of particular importance, CESG should be consulted, and accreditation of the card's physical security features against Common Criteria (ISO 15408) should be considered.

6.3.4 Operating system standards

(a) Objectives

There are a number of commercially available operating systems, each with different strengths and weaknesses. With currently available card platforms, authorities should consider specifying a particular operating system where application portability (the ability to run the same application across multiple types of cards without rewriting) is an issue, or where there is a requirement for a high level of intrinsic operating-system security. Alternatively, and becoming more viable as technology develops, a particular combination of security provision and platform-independent application program interface (API) may be specified.

Application portability may be important where multiple partners are contributing applications (such as in an international project), and should also be considered in the context of the strategy for contract termination. Wherever an application is being developed on behalf of an authority, the choice of operating system and/or platform-independent API should be agreed between the parties. The authority should ensure that the chosen operating system and/or API is in general commercial use and reasonably 'future proof', to avoid the need for porting of the application to an entirely different platform at contract termination.

Software within the card has a great deal to contribute to scheme security. In most of the multi-application card platforms, software implements crypto functions and also handles the isolation of one application from another. The relevant software functions are normally stored in secure Read Only Memory (ROM) or Electrically Erasable Programmable Read Only Memory (EEPROM) in the card's operating system area, and are therefore the responsibility of the card issuer. Some schemes, however, are adequately protected by means of security functions loaded with the application code.

Again, where operating system security is of particular importance, CESG's advice should be sought and the accreditation of the system against the Common Criteria (ISO 15408) should be considered.

(b) Multi-application issues

In most cases, populating the card with applications is the responsibility of the card issuer, with a third-party application provider having access to the management systems in order to block and unblock the provider's application on an individual card basis. Application loading and erasure may be simply implemented using a PC and local reader, but where a large card population and secure data are involved it is more likely that a highly reliable and secure loading network will be used. If a secure network is not used, data encryption and/or the use of digital signatures may be required to implement the loading. Since the card operating system owner has to make arrangements with the loading network operator, signing up for a particular card platform includes making arrangements for application loading and erasure. Card issuing, etc., is handled by the scheme operator or its agent, and includes both procedural items and software elements. As noted previously, all these issues will need to be addressed in detail in any contract between a public sector body and the issuer.

Management systems may be subject to assessment against standard IT and security criteria, but are otherwise normally designed to the scheme manager's requirements.

6.3.5 Application and content standards

(a) Objectives

Application-level standards are critical for interoperability: they govern the interaction between the card and the terminal. The GSM application-level standard, for example, allows an application running on any GSM-compliant card operating system to operate with digital mobile phones that implement the required level of functionality or a higher level.

(b) Standards issues

Card applications usually operate with a command/response model: the terminal sends a command, and the card responds to it. For contact cards, the command protocol is well established. For proximity contactless cards, the standard is still under development, but is intended to stop at a level where the card developer can bridge across to the contact card standards. Contactless cards are also permitted to use non-standard protocols, partly because contactless transactions often have to be optimised for speed (well under half a second). A public sector application that wishes to use the contactless interface but does not need high transaction speed should first consider using the standard protocol.

Data models enshrined in the early ISO/IEC standards did not foresee the multi-application card. Simple configurations where each card application has total control of its data are covered by the existing standards, but practitioners in all areas are asking for a common data area in the card, with a security model giving total control of which application gets to read or alter which data. Several groups are producing draft standards in this area, and they are listed at Annex D.

(c) Preferred standards

A preferred model is presented in Section 7 below.

7 Preferred standards – model for government–citizen interaction

This section presents a preferred model of contents for those cards intended, wholly or in part, to enable citizens to access public services and/or to identify themselves to authorities. The model contains a hierarchy of levels of information. How much of the hierarchy is placed on a particular card will depend on the circumstances of each case. Certain single-function, single-use cards will contain relatively low levels of information, whilst multi-application cards may carry the full complement of components.

Where suitable current or future multiple applications can be identified, a card scheme should be introduced with this possibility in mind, even if in the first instance only a single simple application is included.

At the base of the information hierarchy is information which adds greatly to accessibility or convenience and will be core to most card schemes. Additional optional elements can also be used in cards covering a wide variety of applications. The final group of components comprises individual functions and applications.

Certain single-use public sector applications – such as driving licences – are subject to international agreement as to format, and therefore if issued in smart form may differ from the model set out.

The standards identified are applicable in the following circumstances:

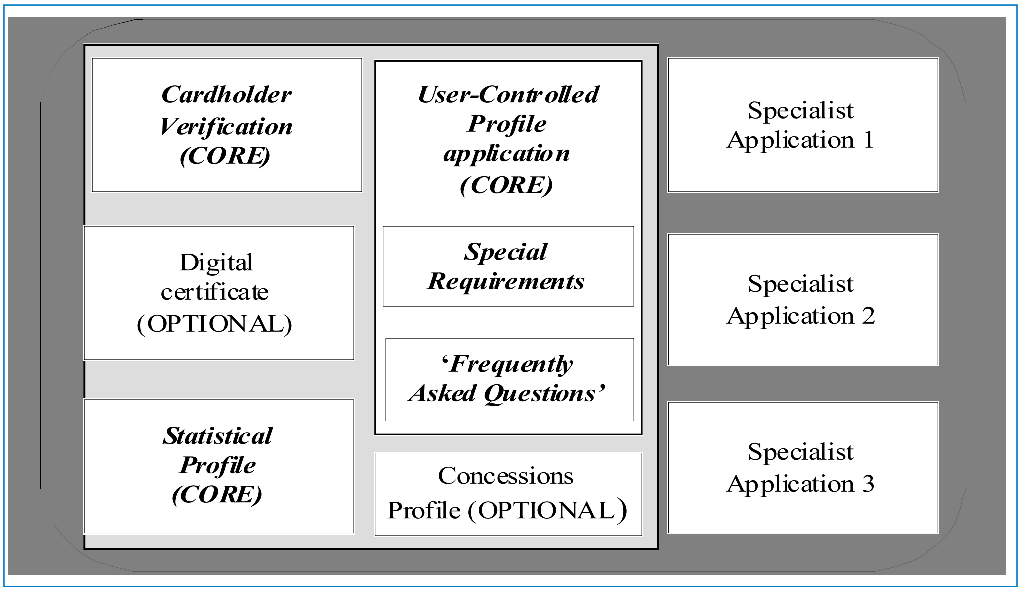
- Features identified as ‘core’ should be incorporated in any card issued by or on behalf of an authority, in accordance with the standards specified, unless they are clearly inapplicable to the uses to which the card will be put.

- It is recommended that these features are also incorporated in any card issued by a third party which is intended to assist members of the public in interacting with the public sector. Availability of the feature and compliance with the specified standard will maximise the number of authorities willing to accept the card. This of course will require an early decision by the card issuer that public sector applications are likely to be appropriate for their card.

- Features identified as ‘optional’ are likely to be of value for public service cards. Where an authority chooses to incorporate any of these optional features, it should be implemented in accordance with the specified standard. Similarly, third parties incorporating such features into their cards are advised to implement them in accordance with the standard in order to maximise usability.

The different elements are illustrated in the following diagram, and set out in the table below.

Figure 1 Different elements


Cardholder Verification (CORE)
User-Controlled Profile application (CORE)
Specialist Application 1
Digital certificate (OPTIONAL)
Special Requirements
Specialist Application 2
'Frequently Asked Questions'
Statistical Profile (CORE)
Specialist Application 3
Concessions Profile (OPTIONAL)

Core components

Component	Purpose	Comments
User-controlled Profile – special requirements	To allow the user to define any preferences for assisting with special requirements. These may include a preference, for example, for a large typeface; an audible interface; wheelchair access; or extra time to pass through a ticket barrier. There is no need to identify users or the nature of their condition or disability for these purposes.	**Core**. Both *content* and *use* under control of the user.
User-controlled Profile – 'frequently asked questions'	To allow the user to store on the card answers to questions which are frequently asked when dealing with public services – such as name, address and date of birth.	Both *content* and *use* are under the control of the user. NB: It is not intended that this will comprise an ID data set to be accessed by all applications.

Component	Purpose	Comments
Cardholder Verification	To identify the legitimate user to the card by means of a PIN, biometric template, or other suitable means or combination of means. This will need to be determined on a case-by-case basis. Biometrics are more secure than PINs, but are more technically complex, less standardised, may be less acceptable to the public, and lack a widespread installed base of readers.	Core where the card holds or gives access to sensitive data or incorporates a digital signature capability
Statistical Profile (non-personal data)	To provide information about the user which is not sufficiently detailed to identify him/her but which is of benefit in identifying public service usage patterns – for example gender, age-group, area of home residence.	Core, but populating this area to be at card-holder's discretion.

Optional generic components

Component	Purpose	Comments
Concessions Profile	To store information about the user's status, which may entitle him/her to concessionary fares, reduced price admission, etc.	
Digital certificate (and private signing key)	To authenticate the cardholder and allow him/her to digitally sign documents.	It should be noted that although the certificate and key are closely related with respect to the efunctionality of the card, the storage and release of these will be handled entirely differently. The digital certificate will be releasable to third parties, whereas the private signing key must remain securely on the card at all times.

Optional case-by-case components		
Component	**Purpose**	**Comments**
Specialist public sector applications	An application placed on the card by an individual public service which need not interoperate with other public services in general and need not therefore be subject to standardisation.	It is the responsibility of individual authorities to consider carefully whether consultation with other authorities is required.
Specialist private sector applications		In these cases, issues of card management, risk allocation, liability, privacy, data protection and public acceptability are likely to require particular care by the authority.

Further details of the preferred data model are contained at Annex A.

Annex A: data model

Data and associated security models

The security model, describing the means of controlling access to the data, is essential to any general data model. ISO/IEC 7816 describes a simple model, appropriate for a single-application card.

Multi-application card operating systems incorporate proprietary models, allowing data sharing between card applications. More recently general models, suitable for porting across card platforms, have been announced by Amex (the Amex Multi-Application Framework) and the Global Chip Alliance. Both of these models are expected to be offered for standardisation in due course.

An EC project named DISTINCT is being standardised by CEN, setting out a simple model describing freely available data stored in the card (e.g. a copy of the information printed on the face of the card, card issuer information, and special needs preferences). This data model does not have an associated security model, but instead relies upon the basic security model in the card to control access from a terminal by means of, for example, a PIN.

In light of this ongoing work, government will work closely with industry on development and implementation of the following model.

Government–citizen interaction

User-controlled profile – 'frequently asked questions'

The user-controlled profile allows the user to place information on the card which will assist service providers to deliver service in a more convenient manner. The 'frequently asked questions' part of the profile contains a set of information which is intended to function as a minimum data set applicable to most public service transactions.

Content
Full name, home address, date of birth and gender of the cardholder.

Information	Standard
Full name	In accordance with the addition to BS 7666 part 3: 1994, proposed by IdeA
Home address	In accordance with BS 7666 part 3: 1994, Spatial data-sets for geographical referencing. Specification for addresses.
Date of birth	In yyyymmdd form
Gender	M or F

Ownership

The data in this section of the card should be owned by the cardholder, who chooses whether to complete it.

Access

Information held in this part of the user-controlled profile should be accessed only with the user's consent – either through having consented to the release of the information when first signing up for a service, or through entering a 'PIN' at the time of release.

User controlled profile – special requirements

Purpose

The 'special requirements' part of the card contains information about a user's special requirements for interfaces, access or assistance. It is intended to help service providers to deliver the best possible service to the disabled and elderly and to meet their obligations under the Disability Discrimination Act 1995.

Content

As defined in EN1332-4. Identification card systems – Man-machine interface – Part 4: Coding of user requirements for people with special needs.

Ownership

The data in this section of the card should be owned by the cardholder, who chooses whether to complete it.

Access

Information held in this part of the user-controlled profile should be accessed only where the circumstances so dictate – i.e. at a service delivery point equipped to cater for special requirements.

Concessions profile

Purpose

The concessions profile contains information about the user's circumstances.

Content

To be agreed – likely to cover age (if under 18 or over 60) and educational status (whether in full-time or part-time education).

Ownership

The data in this section of the card should be owned by the issuing authority.

Access

Information held in this part of the user-controlled profile should be accessed only where the circumstances so dictate – i.e. at a service delivery point offering a concessionary benefit. The user should determine whether to release this information.

Cardholder verification

Purpose

To hold data allowing the card to verify that it is being used by the person to whom it was issued.

Content

An appropriate cardholder verification mechanism – such as a PIN or a biometric template held on the card in one-way encrypted form.

Ownership

This data must be controlled by the issuing authority.

Access

Information held in this part should only be accessed where the circumstances dictate – normally at the service delivery point, where the service provider needs to verify the identity of the card presenter.

Digital certificate and private signing key

Purpose

To identify the cardholder, and to allow him/her to authenticate himself or herself and to sign electronic messages.

Content

The digital certificate should be in accordance with X.509 Version 3 (issued by the International Telecommunications Union (ITU)).

Ownership

The certificate will be issued, and digitally signed by, the issuing party or a trusted third party.

Access

The private signing key should at all times remain on the card, and should not be released to any terminal: hence the card itself must be capable of carrying out a signing operation. No signing operation should be carried out without the cardholder's identity being verified by the card, and the cardholder assenting to the signing operation.

Annex B: applicable standards and specifications - cards and interfaces

Cards should conform to the standards listed below, as indicated under the appropriate heading. In general, the references are undated, indicating that the latest edition should be applied. Where the specific edition is given then later editions may be usable, but with caution. Older editions should never be used.

Standard	Applicable to	Notes
Physical characteristics ISO/IEC 7810 Identification cards – Physical characteristics.	All contact and combination cards.	To ensure that they can be read in a standard reader, all cards should be in ID-1 format as defined in this standard.
Embossing ISO/IEC 7811-1 Identification cards – Recording technique – Part 1: Embossing. ISO/IEC 7811-3 Identification cards – Recording technique – Part 3: Location of embossed characters on ID-1 cards.	Any card where embossing is required.	Embossing should be in the standard location defined herein, for the benefit of the visually impaired and for interoperability reasons, and should conform to the standard in other respects such as height and depth of embossing. It should be noted however that not all smart card readers will accept embossed cards, so the decision to emboss should be taken with care. Note: ISO/IEC 7811-3 will be incorporated into ISO/IEC 7811-1 from the next edition.
Tactile identifiers BS EN 1332-2 Identification card systems – Man-machine interface – Part 2: Dimensions and location of identifier for ID-1 cards.	Where embossing is not used and there is a requirement for the user to present the card in a particular orientation, a tactile identifier should be provided as an aid to those with impaired vision.	Certain card personalisation equipment, unless modified, may have difficulty a tactile processing cards with tactile identifiers of the 'notch' type. Agreement must therefore be reached with the personalisation service provider to use such cards.

Standard	Applicable to	Notes
Identification of issuers		
ISO/IEC 7812–1 Identification cards – Identification of issuers – Part 1: Numbering system ISO/IEC 7812–2 Identification cards – Identification of issuers -Part 2: Application and registration procedures.		
Financial Transaction Cards		
ISO/IEC 7813 Identification cards – Financial transaction cards.	Cards which must carry out banking functions.	Note: ISO/IEC 7813 contains additional information relevant only to magnetic stripes. For physical characteristics it references ISO/IEC 7810 and for IC data content and structure it references ISO/IEC 7816 and ISO 9992.
ISO 9992 Financial transaction cards – Messages between the integrated circuit card and the card-accepting device - Part 1: Concepts and structures; - Part 2: Functions, messages (commands and responses), data elements and structures.		
ISO 10202 Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 1: Card life cycle; - Part 2: Transaction process; - Part 3: Cryptographic key relationships; - Part 4: Secure application modules; - Part 5: Use of algorithms; - Part 6: Cardholder verification; - Part 7: Key management; - Part 8: General principles and overview.		
Integrated circuit(s) cards with contacts		
ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics; – Part 2: Dimensions and location of the contacts; – Part 3: Electronic signals and transmission protocols; – Part 4: Inter-industry commands		

Standard	Applicable to	Notes
for interchange; – Part 5: Numbering system and registration procedure for application identifiers; – Part 6: Inter-industry data elements; – Part 7: Inter-industry commands for Structured Card Query Language (SCQL); - Part 8: Security inter-industry commands; - Part 9: Additional inter-industry commands and security attributes; - Part 10: Electronic signals and answer to reset for synchronous cards; – Part 11: Framework for dynamic handling of multiple applications in integrated circuits cards.	All contact cards .	Note on Part 3: For interoperability purposes, the PPS (protocol and parameters selection) negotiation between cards and terminals is incomplete, and the EMV solution of issuing a warm reset to the card, after which the card must send a 'basic ATR' (answer to reset), is recommended. Note on Part 9: As of October 1999, ISO/IEC 7816-9 is in the final stages of development. ISO/IEC 7816-11 is in the early stages of development.
Contactless integrated circuit(s) cards There are three basic types of contactless card, differentiated nominally by their range of operation but more fundamentally by the detail of their 'air' interface. Of these, the proximity card is likely to be prevalent for public service use.		
Proximity integrated circuit(s) cards (PICC) ISO/IEC 14443 Identification cards – Contactless integrated circuit(s) cards – Proximity cards - Part 1: Physical characteristics; - Part 2: Radio frequency power and signal interface; - Part 3: Initialisation and anticollision; - Part 4: Transmission protocols.	Contactless proximity cards.	Proximity cards are seen as being the volume product for public transport ticketing applications, particularly for mass transit. A number of such products are already well established in closed-system transport applications, including several of the largest urban transit systems in the world. None of these, however, is entirely accommodated by the standard. The set of standards comprises the following parts and defines two basic types of device, designated A and B, to be selected according to the requirements of the application. As of October 1999, ISO/IEC 14443 Parts 1-4 were in the final phases of development.

Other standards

The following standards are listed for information.

Standard	Applicable to	Notes
Close-coupling integrated circuit(s) cards (CICC) ISO/IEC 10536 Identification cards – Contactless integrated circuit(s) cards - Part 1: Physical characteristics; - Part 2: Dimensions and locations of coupling areas; - Part 3: Electronic signals and reset procedures; - Part 4: Answer to reset and transmission protocols.	Contactless cards for use in close-coupling mode (i.e. to be inserted in a slot).	Such cards were originally intended for public telephone payment applications and have not, as yet, seen widespread use. The majority of contactless cards for public service use are expected to be of the proximity type described above. It is possible that this set of standards will be withdrawn before the complete set is issued. As of October 1999, publication of ISO/IEC 10536-4 continued to be delayed.
Vicinity integrated circuit(s) cards (VICC) ISO/IEC 15693 Identification cards – Contactless integrated circuit(s) cards – Vicinity cards - Part 1: Physical characteristics; - Part 2: Air interface and initialisation; - Part 3: Protocols; - Part 4: Registration of applications/issuers.	Vicinity cards, which are typically chosen for remote and 'hands free' applications such as baggage tagging and building occupancy monitoring.	As of October 1999, Parts 1 and 2 were in the final stages of development whilst Parts 3 and 4 were in the early stages of development.

Standard	Applicable to	Notes
Test methods The test methods associated with ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7816, ISO/IEC 10536, ISO/IEC 14443, and ISO/IEC 15693 are found in the following. ISO/IEC 10373 Identification cards – Test methods - Part 1: General characteristics tests; - Part 2: Cards with magnetic stripes; - Part 3: Integrated circuit(s) cards with contacts; - Part 4: Contactless integrated circuit(s) cards; - Part 6: Proximity cards; - Part 7: Vicinity cards.	All card types.	In practice, authorities should specify output-based requirements for performance, interoperability and card life in actual use. The choice of test standards will be a matter for the service provider.

Annex C: Applicable standards and specifications - user interface and terminal equipment

It is recognised that there is a heavy existing investment in terminal equipment and that, in general equipment specifications are application and scheme specific (see Annex D) and not public domain. However, it is recommended that new user interfaces and terminals be designed in accordance with the standards listed below.

Standard	Notes
EN 1332-1 – Identification Card Systems – Man-Machine Interface - Part 1: General Design Principles. EN 1332-2 – Identification Card Systems – Man-Machine Interface - Part 2: Coding of user requirements for special needs. EN1332-3 – Identification Card Systems – Man-Machine Interface - Part 3: Keypads.	Part 2 of EN 1332 defines the information required by equipment that is able to adapt automatically to the user's special needs and preferences.

Authorities are also advised to refer to:

Gill, J: Access Prohibited: Information for Designers of Public Access Terminals. London, RNIB, 1998, available at www.eyecue.co.uk/pats.

Further work in this area continues. In particular, a further part of EN 1332 is expected in March 2002 entitled EN 1332-4 – Identification Card Systems – Man-Machine Interface - Part 4: Provisions for physical disability, including wheelchair access, to card reading devices.

Annex D: A note on application specifications and standards

Although there is standardisation activity in all these areas, there are also scheme specifications that compete more or less successfully with the standards.

Electronic purses

Electronic purse schemes generally operate under the control of card, terminal, and management system specifications, and have associated Type Approval specifications and procedures. Specifications are (except for the Common Electronic Purse Specification) proprietary and not available to the public. Although listed here under applications, these scheme specifications often detail all levels of the scheme.

The following is a non-exhaustive list of purse schemes and their basic documentation:

Visa: VisaCash System Overview, Visa International, 1997

Mondex: Rollout Specifications, Mondex International, 1997

Proton: (no details available)

CEPS: Common Electronic Purse Specification 3 parts, pub. CEPSCO, 1999

Note: CEPS is based on ECBS specifications which in turn are based on the European standard EN1546 Identification card systems - Inter-sector electronic purse.

Purse schemes not trialled in the UK, or not expected to be implemented in the UK, are not listed.

General financial

The major financial scheme specifications are those produced by the EMV consortium (Europay, Mastercard, Visa), its constituent members, and the national operating schemes for bank cards (APACS in the UK), the root document for which is:

EMV'96 Integrated Circuit Card Specification for Payment Systems, V3.1.1, 1998.

An update to this document is in preparation.

The United Kingdom Integrated circuit card Specification (UKIS) debit/credit card specification conforms to EMV'96 V3.0, which particularly does not include encrypted PIN at the point of sale.

Transport

The following European standards already exist:
ENV1545 Identification card systems - Surface transport applications
- Part 1: General data elements;
- Part 2 Transport payment- related data elements;
- Part 3: Tachograph-related data elements;
- Part 4: Driving licence-related data elements;
- Part 5: Freight identification-related data elements;
- Part 6: Vehicle-related data elements.

A new set of European standards is scheduled for the end of 2000, with the following titles (EN numbers will be allocated later):

Identification card systems - Automatic fee collection - Interface definition for IC cards using DSRC;

Identification card systems - Automatic fee collection - Interface definition for IC cards using GSM.

Each of these documents is planned to have four parts, dealing with:
- Physical characteristics, electronic signals and transmission protocols;
- Message requirements;
- Application and security aspects;
- Test procedures.

Telecommunications

In Europe, ETSI produce the major industry specifications and standards. They have done so in collaboration with CEN/CENELEC in the case of machine-readable cards, to produce:
EN 726 Identification card systems - Telecommunications integrated circuit(s) cards and terminals
- Part 1: System overview;
- Part 2: Security framework;
- Part 3: Application independent card requirements;
- Part 4: Application independent card related terminal requirements;
- Part 5: Payment methods;
- Part 6: Telecommunication features;
- Part 7: Security module.

Annex E: membership of the Inter-Departmental Steering Group on Card Technology

Cabinet Office
Central Computer and Telecommunications Agency
Central IT Unit
Central IT Unit (Northern Ireland)
Communications Electronic Security Group
Department for Education and Employment
Department of the Environment, Transport and the Regions
Department of Social Security (Information Technology Services Agency)
Department of Trade and Industry
Driver and Vehicle Licensing Agency
Employment Service
HM Customs & Excise
HM Treasury
Home Office
Inland Revenue
Local Government Association
Ministry of Agriculture, Fisheries and Food
Ministry of Defence
NHS Executive
Office of the Data Protection Registrar
Office for National Statistics
Scottish Executive
Southampton City Council
Southend-on-Sea Borough Council
United Kingdom Passport Agency
Welsh Office